IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application:	:	Group Art Unit: 2132
Frederic G. Thiele et al.	:	Examiner: Venkatanaray Perungavoor
Serial No.: 10/650,440	:	IBM Corporation
Filed: 08/27/2003	:	Intellectual Property Law
Confirmation No. 7247	:	Department SHCB/040-3
Title: SYSTEM, METHOD AND PROGRAM PRODUCT FOR DETECTING UNKNOWN COMPUTER ATTACKS	:	1701 North Street Endicott, NY 13760

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

I. Real Party in Interest

International Business Machines Corporation is the real party in interest.

II. Related Appeals and Interferences

There are no related appeals or interferences.

III. Status of Claims

Claims 1-16 and 21-24 are pending and Final Rejected.

Claims 17-20 were canceled.

IV. Status of Amendments

There were no amendments filed subsequent to Final Rejection.

V. Summary of Claimed Subject Matter

Support for each claim element is indicated in plain brackets [ ].

Claim 1 recites a computer program product [Program tool 30. Figure 1. Page 7 line 25 to Page 8 line 1 and Page 8 lines 12-20. Figure 2] for automatically determining if a packet is a new, exploit candidate. First program instructions determine if the packet is a known exploit or portion thereof. [Decision 100 of Figure 2. Page 8 lines 13-15]. Second program instructions determine if the packet is addressed to a broadcast IP address of a network. [Decision 106 of Figure 2. Page 8 lines 21-23] Third program instructions determine if the packet is network administration traffic. [Decision 110 of Figure 2. Page 9 lines 10-14.] Fourth program instructions are responsive to the packet being a known exploit or portion thereof, addressed to a broadcast IP address of a network, or network administration traffic, to determine that the packet is not a new, exploit candidate. [Decision 100, yes branch, Decision 106, yes branch, Decision 110, yes branch, step 102. Page 8 lines 12-20. Page 9 lines 6-8.] Fifth program instructions are responsive to the packet not being a known exploit or portion thereof, addressed to a broadcast IP address of a network, network administration traffic or another type of traffic known to be benign, to determine and report that the packet is a new, exploit candidate. [Step 124 of Figure 2. Page 10 lines 2-10.]

Claim 13 recites a computer system [Program tool 30 executing in computer 12. Figure 1. Page 7 line 25 to Page 8 line 1 and Page 8 lines 12-20. Figure 2] for automatically determining if a packet is a new, exploit candidate. There are means for determining if the packet is a known exploit or portion thereof. [Decision 100 of Figure 2. Page 8 lines 13-15]. There are means for determining if the packet is addressed to a broadcast IP address of a network. [Decision 106 of Figure 2. Page 8 lines 21-23] There are means for determining if the packet is network administration traffic. [Decision 110 of Figure 2. Page 9 lines 10-14.] There

are means, responsive to the packet being the known exploit or portion thereof, addressed to the broadcast IP address of said network, or network administration traffic, for determining that the packet is not a new, exploit candidate. [Decision 100, yes branch, Decision 106, yes branch, Decision 110, yes branch, step 102. Page 8 lines 12-20. Page 9 lines 6-8.] There are means, responsive to the packet not being a known exploit or portion thereof, addressed to the broadcast IP address of the network, network administration traffic or another type of traffic known to be benign, for determining and reporting that the packet is a new, exploit candidate. [Step 124 of Figure 2. Page 10 lines 2-10.]

Claim 21 recites a computer program product [Program tool 30. Figure 1. Page 7 line 25 to Page 8 line 1 and Page 8 lines 12-20. Figure 2] for automatically determining if a packet is a new, exploit candidate. First program instructions determine if the packet is a known exploit or portion thereof. [Decision 100 of Figure 2. Page 8 lines 13-15]. Second program instructions determine if the packet is addressed to a broadcast IP address of a network. [Decision 106 of Figure 2. Page 8 lines 21-23] Third program instructions determine if the packet has a protocol listed in a list of protocols assumed to be harmless broadcast traffic. [Decision 108 of Figure 2. Page 9 line 18 to Page 10 line 2.] Fourth program instructions determine if the packet is network administration traffic. [Decision 110 of Figure 2. Page 9 lines 10-14.] Fifth program instructions are responsive to the packet being a known exploit or portion thereof, addressed to a broadcast IP address of a network or network administration traffic or having a protocol listed in a list of protocols assumed to be harmless broadcast traffic, to determine that the packet is not a new, exploit candidate. [Decision 100, yes branch, Decision 106, yes branch, Decision 108, yes branch, Decision 110, yes branch, Decision 120, yes branch, step 102. Page 8 lines 12-20. Page 9 lines 6-8.] Sixth program instructions are responsive to the packet not being a known exploit or portion thereof, addressed to a broadcast IP address of a network or network administration traffic and not having a protocol listed in a list of protocols assumed to be harmless broadcast traffic, to determine and report that said packet is a new, exploit candidate. [Step 124 of Figure 2. Page 10 lines 2-10.]

The structure, material or acts corresponding to means plus function elements are indicated in stylized brackets { }.

Claim 13. A computer system for automatically determining if a packet is a new, exploit candidate, said system comprising:

means for determining if said packet is a known exploit or portion thereof; {Decision 100 of Figure 2. Page 8 lines 13-15}.

means for determining if said packet is addressed to a broadcast IP address of a network; and {Decision 106 of Figure 2. Page 8 lines 21-22}

means for determining if said packet is network administration traffic; {Decision 110 of Figure 2. Page 9 lines 10-14.} wherein

means, responsive to said packet being said known exploit or portion thereof, addressed to said broadcast IP address of said network, or network administration traffic, for determining that said packet is not a new, exploit candidate; {Decision 100, yes branch, Decision 106, yes branch, Decision 110, yes branch, step 102.} and

means, responsive to said packet not being a known exploit or portion thereof, addressed to said broadcast IP address of said network, network administration traffic or another type of traffic known to be benign, for determining and reporting that said packet is a new, exploit candidate. {Step 124 of Figure 2. Page 10 lines 2-4.}

Claim 14. A computer system as set forth in claim 13 further comprising:

means for determining if said packet is web crawler traffic; {Decision 114 and Page 9 lines 16-18} and wherein

said means for determining that said packet is not a new, exploit candidate determines that said packet is not a new exploit candidate if said packet is web crawler traffic. {Decision 114, yes branch and step 102}.

VI. Grounds of Rejection to be Reviewed Upon Appeal

Claims 1-2, 4-5, 7, 12-15 and 21-22 were rejected under 35 USC 103 based on US Patent Publication 2003/0145228 to Suuronen et al. and US Patent Publication 2002/0116512 to Amit et al.

Claims 3, 8-11 and 24 were rejected under 35 USC 103 based on Suuronen et al., Amit et al. and US Patent 6,853,619 to Grenot.

Claims 6, 16 and 23 were rejected under 35 USC 103 based on Suuronen et al, Amit et al. and US Patent Publication 2002/0131369 to Hasegawa et al.

VII. Argument

A claim cannot be obvious under 35 USC 103 unless (a) there is a reason that a person of ordinary skill in the art would have combined the references, and (b) all the claim elements are taught or suggested by the prior art. See In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438, 1443 (Fed Cir. 1991) and KSR Int'l Co. v. Teleflex, Inc., No. 04-1350 (USSC 30 April 2007).

Rejection of Claims 1, 4-5, 7, 12-13, 15, and 17 under 35 USC 103 based on Suuronen et al. and Amit et al.

Independent Claim 1 was rejected under 35 USC 103 based on Suuronen et al. and Amit et al. Appellants respectfully traverse this rejection based on the following.

Claim 1 recites a computer program product for automatically determining if a packet is a new, exploit candidate. First program instructions determine if the packet is a known exploit or portion thereof. Second program instructions determine if the packet is addressed to a broadcast IP address of a network. Third program instructions determine if the packet is network administration traffic. Fourth program instructions are responsive to the packet being a known exploit or portion thereof, addressed to a broadcast IP address of the network, or network administration traffic, to determine that the packet is not a new, exploit candidate. Fifth program instructions are responsive to the packet not being a known exploit or portion thereof, addressed to a broadcast IP address of the network, network administration traffic or another type of traffic known to be benign, to determine and report that the packet is a new, exploit candidate.

Suuronen et al. disclose a virus scanning engine, and a bypass/screening system to identify certain packets such as audio and video data streams (packets called the "first type" in Suuronen et al.), which cannot be viruses and should bypass the virus scanning engine to increase throughput. The objective is to avoid the overhead and delays involved in virus screening of audio and video data streams, which need to reach their destination in real time, and are not viruses. Suuronen et al. also state that packets of the "first type" include "other real time data which cannot contain viruses are not delayed by the virus scanning engine." However, Suuronen et al. fail to disclose the second and third program instructions of claim 1 which determine if the packet is addressed to a broadcast IP address of a network or network administrative traffic. Suuronen et al. fail to disclose the fourth program instructions of claim 1 which are responsive to the packet being a known exploit or portion thereof, addressed to a broadcast IP address of the network, or network administration traffic, to determine that the packet is not a new, exploit candidate. Suuronen et al. fail to disclose the fifth program instructions which are responsive to the packet not being a known exploit or portion thereof, addressed to a broadcast IP address of the network, network administration traffic or another type of traffic known to be benign, to determine and report that the packet is a new exploit candidate.

Also, Suuronen et al. do not teach or suggest identification of new, exploit candidates as specified in the fourth and fifth program instructions of claim 1. Rather, Suuronen et al. merely determine which packets should be passed to (or conversely bypass) a virus scanning engine "with virus detection criteria specified by virus detection database 24." See Suuronen et al. Paragraph 0021. Thus, Suuronen et al. determine if the packets contain a known virus **signature**. If a packet passes through the virus scanning engine of Suuronen, this means that the packet is presumed not to be a virus. The virus scanning engine of Suuronen et al. does not attempt to identify new, exploit candidates that do not exist in the virus detection database.

Amit et al. do not fill the many gaps of Suuronen et al. Amit et al. are concerned with simulating a web browser by monitoring TCP/IP data packets routed through a communication line and filtering relevant requests and responses relating to a given IP address. These requests and responses are analyzed and sorted according to their type and content. Based on the analysis, a probe terminal identifies all relevant data transactions relating to the navigation process of the given terminal. The probe terminal activates a virtual browser simulating the processing of identified data transactions to create navigation presentations similar to the real navigation as seen by the user of the given terminal.

Amit et al. disclose a method of tracking a network communication line by a network probe terminal simulating a browser activity of a terminal comprising the steps of accessing the network communication line, tracing TCP/IP data packets routed through the communication line, selecting TCP/IP data packets relating to a given IP address, selecting from the identified data packets current requests for new connections, selecting from the identified data packets current web page components indicating new addressees, dividing the new navigation components into two categories, embedded objects or frames, hyperlinks, dividing the original requests into original request matching true the new components, or original request failing to match any new connection components and belonging to HTTP or POST type as primary requests, original requests matching the false components as secondary requests, selecting from identified data packets, HTML data files relating to primary requests, generating virtual secondary requests according to the respective secondary responses, selecting from identified data packets responses relating to secondary virtual requests and simulating web page

presentation on the terminal agent according to the respective secondary responses. See Summary of Amit et al. Paragraph 0017.

However, Amit et al. are not concerned with identifying new exploits. Amit et al. do not fill any of the foregoing gaps of Suuronen et al. Amit et al. fail to disclose the second and third program instructions of claim 1 which determine if the packet is addressed to a broadcast IP address of a network or network administrative traffic as part of a program (or system) for identifying new exploits. Thus, Amit et al. fail to disclose the fourth program instructions of claim 1 which are responsive to the packet being a known exploit or portion thereof, addressed to a broadcast IP address of the network, or network administration traffic, to determine that the packet is not a new, exploit candidate. Amit et al. fail to disclose the fifth program instructions which are responsive to the packet not being a known exploit or portion thereof, addressed to a broadcast IP address of the network, network administration traffic or another type of traffic known to be benign, to determine and report that the packet is a new exploit candidate. Therefore, Suuronen et al. and Amit et al. in combination do not teach or suggest the foregoing features of claim 1.

Moreover, it would not have been obvious to combine Suuronen et al. with Amit et al. and there would be no reason to combine Suuronen et al. with Amit et al. because they address much different tasks and problems. Suuronen et al. are concerned with a virus scanning engine, and a bypass/screening system to identify certain packets such as audio and video data streams which cannot be viruses and should bypass the virus scanning engine. Amit et al. are concerned with monitoring network traffic to simulate browser activity and thereby simulate navigation presentations similar to the real navigation as seen by the user of the terminal. See Abstract and Paragraphs 0038 of Amit et al. These are much different technologies involving different technicians, and there would be no reason to combine these two documents.

Independent claim 13 distinguishes over the prior art for the same reasons that claim 1 distinguishes thereover.

Rejection of Claims 2 and 14 under 35 USC 103

based on Suuronen et al. and Amit et al.

Claim 2 depends on claim 1 and recites sixth program instructions to determine if the packet is web crawler traffic. In addition, the fourth program instructions are responsive to the packet being a known exploit or portion thereof, addressed to a broadcast IP address of a network, network administration traffic or web crawler traffic, to determine that the packet is not a new, exploit candidate. In addition, the fifth program instructions are responsive to the packet not being a known exploit or portion thereof, addressed to a broadcast IP address of a network, network administration traffic or web crawler traffic, to determine that the packet is a new, exploit candidate. Neither Suuronen et al. nor Amit et al. teach or suggest these features of claim 2. While Suuronen et al. teach a firewall to identify "data packets which cannot contain viruses", Suuronen et al. do not teach the foregoing program instructions of claim 2. Amit et al. are concerned with simulating a web browser and do not fill this gap of Suuronen et al.

Moreover, it would not have been obvious to combine Suuronen et al. with Amit et al. and there would be no reason to combine Suuronen et al. with Amit et al. as explained above with reference to claim 1.

Claim 14 depends on claim 13 and distinguishes over the prior art for the same reasons that claim 2 distinguishes over the prior art.

Rejection of Claim 9 under 35 USC 103
based on Suuronen et al., Amit et al. and Grenot

Claim 9 depends on claim 1. In addition, claim 21 recites another criteria to determine whether the packet is a new, exploit candidate, i.e. whether the packet has a protocol listed in a list of protocols assumed to be harmless broadcast traffic. This other criteria is not taught or suggested by Suuronen et al., Amit et al. and Grenot, individually or in combination.

Grenot teaches a system and method for measuring transfer durations and loss rates of data packets in high volume telecommunications networks. Grenot discloses that an identification signature for each data packet is calculated. Grenot also discloses that "each packet is subjected to a classification operation 44. Criteria for classification are typically those that are conventionally retained to identify flows between networks and sub-networks (such as IP network subaddresses), flows between end equipment (such as IP addresses), flows between applications (such as IP addresses and UDP/TCP transport addresses), etc. Each packet is then identified by combining all or part of the elements: class, date signature." Column 6 lines 26-34. However, Grenot does not disclose or even suggest a program for determining new, exploit candidates. Rather, Grenot is concerned with measuring transfer durations and loss rates of data packets in high volume telecommunications networks. Grenot does not disclose any algorithm for determining new, exploit candidates. Grenot does not disclose the algorithm of claim 1 for determining new, exploit candidates. Even though Grenot identifies various IP addresses associated with a packet, Grenot does not perform the program operations of claim 1 to determine new, exploit candidates. Grenot fail to disclose program instructions of claim 1 which determine whether a packet is a new, exploit candidate based on whether the packet is a known exploit or portion thereof, addressed to a broadcast IP address of the network or network administration traffic or has a protocol listed in a list of protocols assumed to be harmless network broadcast traffic.

Moreover, it would not have been obvious to combine Suuronen et al. with Amit et al. and Grenot and there would be no reason to combine Suuronen et al. with Amit et al. and Grenot

because they address much different tasks and problems. Suuronen et al. are concerned with a virus scanning engine, and a bypass/screening system to identify certain packets such as audio and video data streams which cannot be viruses and should bypass the virus scanning engine. Amit et al. are concerned with monitoring network traffic to simulate browser activity and thereby simulate navigation presentations similar to the real navigation as seen by the user of the terminal. See Abstract and Paragraphs 0038 of Amit et al. Grenot teaches a system and method for measuring transfer durations and loss rates of data packets in high volume telecommunications networks. These are much different technologies involving different technicians, and there would be no reason to combine these three documents.

Rejection of Claims 3, 8, 10-11 and 24 under 35 USC 103
based on Suuronen et al., Amit et al. and Grenot

Claims 3, 8 and 10-11 depend on claim 1 and therefore distinguish over Suuronen et al. and Amit et al. for the same reasons that claim 1 distinguishes thereover. Claim 24 depends on claim 21 and therefore distinguishes over Suuronen et al. and Amit et al. for the same reasons that claim 21 distinguishes thereover. Grenot does not fill the foregoing gaps of Suuronen et al. and Amit et al. relative to base claims 1 and 21.

Grenot teaches a system and method for measuring transfer durations and loss rates of data packets in high volume telecommunications networks. Grenot discloses that an identification signature for each data packet is calculated. Grenot also discloses that "each packet is subjected to a classification operation 44. Criteria for classification are typically those that are conventionally retained to identify flows between networks and sub-networks (such as IP network subaddresses), flows between end equipment (such as IP addresses), flows between applications (such as IP addresses and UDP/TCP transport addresses), etc. Each packet is then identified by combining all or part of the elements: class, date signature." Column 6 lines 26-34. However, Grenot does not disclose or even suggest a program for determining new, exploit candidates. Rather, Grenot is concerned with measuring transfer durations and loss rates of data packets in high volume telecommunications networks. Grenot does not disclose any algorithm for determining new, exploit candidates. Grenot does not disclose the algorithm of claim 1 for

determining new, exploit candidates. Even though Grenot identifies various IP addresses associated with a packet, Grenot does not perform the program operations of claim 1 to determine new, exploit candidates. Grenot fail to disclose program instructions of claim 1 which determine whether a packet is a new, exploit candidate based on whether the packet is a known exploit or portion thereof, addressed to a broadcast IP address of the network or network administration traffic or has a protocol listed in a list of protocols assumed to be harmless network broadcast traffic.

Moreover, it would not have been obvious to combine Suuronen et al. with Amit et al. and Grenot and there would be no reason to combine Suuronen et al. with Amit et al. and Grenot because they address much different tasks and problems. Suuronen et al. are concerned with a virus scanning engine, and a bypass/screening system to identify certain packets such as audio and video data streams which cannot be viruses and should bypass the virus scanning engine. Amit et al. are concerned with monitoring network traffic to simulate browser activity and thereby simulate navigation presentations similar to the real navigation as seen by the user of the terminal. See Abstract and Paragraphs 0038 of Amit et al. Grenot teaches a system and method for measuring transfer durations and loss rates of data packets in high volume telecommunications networks. These are much different technologies involving different technicians, and there would be no reason to combine these three documents.

Rejection of Claim 21 under 35 USC 103
based on Suuronen et al. and Amit et al.

Independent claim 21 distinguishes over the prior art for the same reasons that claim 1 distinguishes thereover. In addition, claim 21 recites another criteria to determine whether the packet is a new, exploit candidate, i.e. whether the packet has a protocol listed in a list of protocols assumed to be harmless broadcast traffic. This other criteria is not taught or suggested by Suuronen et al. and Amit et al. Moreover, this other criteria is not taught or suggested by Grenot and there would be no reason to combine Suuronen et al. with Amit et al. and Grenot as explained above with reference to dependent claim 9.

Moreover, it would not have been obvious to combine Suuronen et al. with Amit et al. and there would be no reason to combine Suuronen et al. with Amit et al. as explained above with reference to claim 1.

Rejection of Claim 22 under 35 USC 103
based on Suuronen et al. and Amit et al.

Claim 22 depends on claim 21 and recites sixth program instructions to determine if the packet is web crawler traffic. In addition, the fourth program instructions are responsive to the packet being a known exploit or portion thereof, addressed to a broadcast IP address of a network, network administration traffic or web crawler traffic or having a protocol listed in a list of protocols assumed to be harmless broadcast traffic, to determine that the packet is not a new, exploit candidate. In addition, the fifth program instructions are responsive to the packet not being a known exploit or portion thereof, addressed to a broadcast IP address of a network, network administration traffic or web crawler traffic or other traffic known to be benign or having a protocl listed in a list of protocls assumed to be harmless broadast traffic, to determine that the packet is a new, exploit candidate. Neither Suuronen et al. nor Amit et al. teach or suggest these features of claim 22. While Suuronen et al. teach a firewall to identify "data

packets which cannot contain viruses", Suuronen et al. do not teach the foregoing program instructions of claim 22. Amit et al. do not fill this gap either.

Moreover, it would not have been obvious to combine Suuronen et al. with Amit et al. and there would be no reason to combine Suuronen et al. with Amit et al. as explained above with reference to claim 1.

Rejection of Claims 6, 16 under 35 USC 103
based on Suuronen et al., Amit et al. and Hasegawa et al.

Claim 6 depends on claim 1 and therefore distinguishes over Suuronen et al. and Amit et al. for the same reasons that claim 1 distinguishes thereover. Hasegawa et al. disclose a network traffic monitoring system comprising a plurality of active traffic monitors each tapping a physical line on a network and analyzing traffic, and a central manager collecting data from the plurality of active traffic monitors. Hasegawa et al. do not fill the gaps of Suuronen et al. and Amit et al. noted above in relation to claim 1.

Claim 16 depends on claim 13 and therefore distinguishes over Suuronenet al. and Amit et al. for the same reasons that claim 13 distinguishes thereover. Hasegawa et al. disclose a network traffic monitoring system comprising a plurality of active traffic monitors each tapping a physical line on a network and analyzing traffic, and a central manager collecting data from the plurality of active traffic monitors. Hasegawa et al. do not fill the gaps of Suuronen et al. and Amit et al. noted above in relation to claim 13.

Rejection of Claim 23 under 35 USC 103

based on Suuronen et al., Amit et al. and Hasegawa et al.

Claim 23 depends on claim 21 and therefore distinguishes over Suuronenet al. and Amit et al. for the same reasons that claim 21 distinguishes thereover. Hasegawa et al. disclose a network traffic monitoring system comprising a plurality of active traffic monitors each tapping a physical line on a network and analyzing traffic, and a central manager collecting data from the plurality of active traffic monitors. Hasegawa et al. do not fill the gaps of Suuronen et al. and Amit et al. noted above in relation to claim 21.

Based on the foregoing, Appellants request that all rejections under 35 USC 103 be reversed.

Respectfully submitted,

Dated: 08/13/07

Telephone: 607-429-4368

Fax No.: 607-429-4119

/Arthur J. Samodovitz/

Arthur J. Samodovitz

Reg. No. 31,297

VIII. CLAIMS APPENDIX

1. A computer program product for automatically determining if a packet is a new, exploit candidate, said program product comprising:

a computer readable medium;

first program instructions to determine if said packet is a known exploit or portion thereof;

second program instructions to determine if said packet is addressed to a broadcast IP address of a network; and

third program instructions to determine if said packet is network administration traffic; fourth program instructions, responsive to said packet being a known exploit or portion thereof, addressed to a broadcast IP address of a network, or network administration traffic to determine that said packet is not a new, exploit candidate; and

fifth program instructions, responsive to said packet not being a known exploit or portion thereof, addressed to a broadcast IP address of a network, network administration traffic or another type of traffic known to be benign, to determine and report that said packet is a new, exploit candidate; and wherein

said first, second, third, fourth and fifth program instructions are embodied on said medium.

2. A computer program product as set forth in claim 1 further comprising:

sixth program instructions to determine if said packet is web crawler traffic; and wherein

said fourth program instructions are responsive to said packet being a known exploit or portion thereof, addressed to a broadcast IP address of a network, network administration traffic or web crawler traffic, to determine that said packet is not a new, exploit candidate; and

said fifth program instructions are responsive to said packet not being a known exploit or portion thereof, addressed to a broadcast IP address of a network, network administration traffic or web crawler traffic, to determine that said packet is a new, exploit candidate; and

said sixth program instructions are embodied on said medium.

3. A computer program product as set forth in claim 1 wherein said first program instructions determine if said packet is a known exploit or portion thereof by searching said packet for a known signature of said known exploit.

4. A computer program product as set forth in claim 1 wherein said first program instructions determine if said packet is a known exploit by comparing an identity of said packet to one or more identities, sent by an intrusion detection system, of respective packet(s) which said intrusion detection system determined to contain a known exploit or portion thereof.

5. A computer program product as set forth in claim 1 wherein said packet was received by a computing device at an unused IP address, and said program product is executed at said computing device.

6. A computer program product as set forth in claim 1 further comprising:

sixth program instructions, responsive to said fifth program instructions determining that said packet is a new exploit candidate, to determine a signature of said packet or a sequence of packets including the first said packet, and report said new exploit candidate and said signature to an administrator; and wherein

said sixth program instructions are embodied on said medium.

7. A computer program product as set forth in claim 6 wherein if said fourth program instructions determine that said packet is not a new, exploit candidate, then a signature of said packet or a sequence of packets including said first packet is not determined.

8. A computer program product as set forth in claim 1 wherein said second program instructions determine if said packet is addressed to a broadcast IP address of said network by comparing a destination IP address of said packet to a gateway IP address and netmask of said network which identifies a broadcast IP address of said network.

9. A computer program product as set forth in claim 1 wherein:

said second program instructions also determine if said packet has a protocol listed in a list of protocols assumed to be harmless network broadcast traffic

said fourth program instructions is responsive to said packet being a known exploit or portion thereof, addressed to a broadcast IP address of a network, network administration traffic or having a protocol listed in a list of protocols assumed to be harmless network broadcast traffic, to determine that said packet is not a new, exploit candidate; and

said fifth program instructions is responsive to said packet not being a known exploit or portion thereof, addressed to a broadcast IP address of a network or network administration traffic and not having a protocol listed in a list of protocols assumed to be harmless network broadcast traffic, to determine and report that said packet is a new, exploit candidate.

10. A computer program product as set forth in claim 1 wherein said third program instructions determine if said packet is network administration traffic by comparing an IP protocol and IP address of said packet to a list of combinations of IP protocols and IP addresses assumed to be network administration traffic.

11. A computer program product as set forth in claim 2 wherein said sixth program instructions determine if said packet is web crawler traffic by comparing an IP address of said packet to a list of IP addresses of known web crawlers.

12. A computer program product as set forth in claim 1 further comprising sixth program instructions, responsive to said packet not being a known exploit, network broadcast traffic, addressed to a broadcast IP address of a network or other type of traffic known to be benign, to identify a sequence of packets including the first said packet, said sequence of packets being a new, exploit candidate; and wherein

said sixth program instructions are embodied on said medium.

13. A computer system for automatically determining if a packet is a new, exploit candidate, said system comprising:

means for determining if said packet is a known exploit or portion thereof;

means for determining if said packet is addressed to a broadcast IP address of a network; and

means for determining if said packet is network administration traffic; wherein

means, responsive to said packet being said known exploit or portion thereof, addressed to said broadcast IP address of said network, or network administration traffic, for determining that said packet is not a new, exploit candidate; and

means, responsive to said packet not being a known exploit or portion thereof, addressed to said broadcast IP address of said network, network administration traffic or another type of traffic known to be benign, for determining and reporting that said packet is a new, exploit candidate.

14. A computer system as set forth in claim 13 further comprising:

means for determining if said packet is web crawler traffic; and wherein

said means for determining that said packet is not a new, exploit candidate determines that said packet is not a new exploit candidate if said packet is web crawler traffic.

15. A computer system as set forth in claim 13 wherein said packet was received by said computer system in said network at an unused IP address.

16. A computer system as set forth in claim 13 further comprising means, responsive to said packet not being a new exploit candidate, for determining a signature of said packet or a sequence of packets including the first said packet, and reporting said new, exploit candidate and said signature to an administrator.

Claims 17-20 (Canceled)

21. A computer program product for automatically determining if a packet is a new, exploit candidate, said program product comprising:

a computer readable medium;

first program instructions to determine if said packet is a known exploit or portion thereof;

second program instructions to determine if said packet is addressed to a broadcast IP address of a network;

third program instructions to determine if said packet has a protocol listed in a list of protocols assumed to be harmless broadcast traffic;

fourth program instructions to determine if said packet is network administration traffic;

fifth program instructions, responsive to said packet being a known exploit or portion thereof, addressed to a broadcast IP address of a network or network administration traffic or having a protocol listed in a list of protocols assumed to be harmless broadcast traffic, to determine that said packet is not a new, exploit candidate; and

sixth program instructions, responsive to said packet not being a known exploit or portion thereof, addressed to a broadcast IP address of a network or network administration traffic and not having a protocol listed in a list of protocols assumed to be harmless broadcast traffic, to determine and report that said packet is a new, exploit candidate; and wherein

said first, second, third, fourth, fifth and sixth program instructions are embodied on said medium.

22. A computer program product as set forth in claim 21 further comprising:

seventh program instructions to determine if said packet is web crawler traffic; and wherein

said fifth program instructions are responsive to said packet being a known exploit or portion thereof, addressed to a broadcast IP address of a network, network administration traffic or web crawler traffic or having a protocol listed in a list of protocols assumed to be harmless broadcast traffic, to determine that said packet is not a new, exploit candidate; and

said sixth program instructions are responsive to said packet not being a known exploit or portion thereof, addressed to a broadcast IP address of a network, network administration traffic or web crawler traffic or other traffic known to be benign or having a protocol listed in a list of protocols assumed to be harmless broadcast traffic, to determine that said packet is a new, exploit candidate; and

said seventh program instructions are embodied on said medium.

23. A computer program product as set forth in claim 21 further comprising:

seventh program instructions, responsive to said sixth program instructions determining that said packet is a new, exploit candidate, to determine a signature of said packet or a sequence of packets including the first said packet, and report said new, exploit candidate and said signature to an administrator; and wherein

said seventh program instructions are embodied on said medium.

24. A computer program product as set forth in claim 21 wherein said second program instructions determine if said packet is addressed to a broadcast IP address of said network by comparing a destination IP address of said packet to a gateway IP address and netmask of said network which identifies a broadcast IP address of said network.

IX. Evidence Appendix

There is no evidence entered or relied upon in this Appeal.

X. Related Proceedings Appendix

There are no related proceedings, and therefore, no copies of such decisions to attach.